Information & Security

Published since 1998

I. Gaidarski & A. Madzharov
vol. 55, no. 3 (2024): 261-272
https://doi.org/10.11610/isij.5546

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Applying a New Approach to Consider the Human Factor in the Design of Information Security Systems

Ivan Gaidarski (✉) and ***Anastas Madzharov***

Institute of Robotics "St. Ap. and Gospeller Matthew," Bulgarian Academy of Sciences, Sofia, Bulgaria, http://ir.bas.bg

Abstract:

A primary task of information security in modern organisations is to ensure the safety of their information assets. The most effective method is to develop and implement an information security system (ISS) that is designed for a specific organisation and meets the organisation-specific requirements. Two methods for creating ISS are considered in the article – development of a complex ISS through systems analysis and the authors' method for the development of organisational ISS. These methods consider different viewpoints on the system. An example is given with Information Security Viewpoint and related concepts such as "Incident," "Breach," "Vulnerability," "Threats," "Threat Sources," and a "Threat Agent" with taking the human factor in account. As the behaviour of employees in relation to the adopted information security policy cannot be predicted, it is necessary to foresee some measures in the process of designing the system.

Article Info:

Received: 19 Sep 2024
Revised: 22 Oct 2024
Online: 04 Nov 2024

Keywords:

information security system, human factors, vulnerability, threat, agent, insider threat

Creative Commons BY-NC 4.0

✉ E-mail: ivangaidarski@ir.bas.bg; a.madzharov@ir.bas.bg

Introduction

Modern organizations, regardless of their size and structure, handle a huge amount of information - patents, commercial information such as customer and supplier lists, intellectual property, and know-how.[1] This information forms their competitive advantage and is vital to their existence. It can be said that such information is the most valuable asset they have. Regardless of its form - electronic or physical, it is vital for organizations to protect it from tampering, leakage, or alteration. In addition to traditional external threats, information assets must also be protected from inside threats. Such are employees with access to sensitive information and suppliers of raw materials, as well as services having access to the organization's resources. Ensuring the safety of assets is the task of Information Security (IS). For this purpose, each information asset must be considered alongside the risk associated with its loss, as well as with its value. Modern organizations have specific business models. They must cover different normative and regulatory requirements, as well as the respective requirements for IS. For this reason, it is not appropriate to use universal IS solutions. The most effective method is to develop and implement an information security system (ISS) that is designed for the specific organization, with detailed requirements for its needs. Designing an effective ISS is vital for national security, critical infrastructure, and governments.[2]

Research Question

Traditional cybersecurity methods consider the human factor as a threat agent entirely external to the system. The current state of information security clearly shows that a significant part of threats is hidden and located inside the protected network of the organization. In this article, we consider applying a new approach to the human factor in the design of information security systems as internal to an organization. For the purposes of the article, we limit ourselves to precisely this internal threat, which traditional information security systems ignore.

Methods

In the present study, we use the following two methods: Development of complex ISS through systems analysis and method for development of ISS in organisations.

Development of Complex ISS through Systems Analysis

System analysis is the process of clarifying the problems that the designed ISS must solve, unambiguously defining the goals, and making an assessment of the value of the system in relation to the protected assets - risk analysis. The next stage is the determination of priorities in the development process, including the selection of the development methodology and the relevant technologies to satisfy the system requirements.[3, 4]

System analysis involves the identification of several main components and relationships between them:

1.Problem area (PA) - the area in which ISS problems are solved;

2.Implementation environment - the conditions under which the ISS is implemented;

3.Problem – design and implementation of ISS, solving a specific problem in a specific environment;

4.Stages – The different stages of the ISS development;

5.Constructing various models in the ISS design process;

6.Transformation of the models;

The stages of ISS development include:

1.Defining the requirements for the ISS, based on the requirements of the various participants;

2.Determining possible risks according to users' understanding;

3.Analysis - research of the PA from different perspectives;

4.Design of the ISS structure;

5.Clarification of the processes in the ISS;

6.Implementation – aligning ISS technologies, structure and processes with the chosen development environment.

For the realization of the necessary ISS, the following models are constructed:

1.Risk model, based on the estimated cost of protecting information and infrastructure assets and their cost;

2.Model of the ISS area, based on analysis of the PA;

3.Project model - architecture and functionality of ISS;

4.Implementation model of the designed ISS - depends on the selected platform and the conditions under which the ISS operates.

Method for Development of Organisational ISS

A method for designing ISS in organisations, developed by the author (ig), aims to bring together the requirements of different stakeholders.[5,6] The method uses the principles of conceptual modelling through which different viewpoints can be represented. The method ensures the unification of communication between different participants.

The following phases (Fig.1) are characteristic of the method:

1.Constructing a framework for the architectural description of the ISS. The framework is formed based on IEEE 1471 [7, 8] and IEEE 42010 [9] standards.

2.Determining the requirements to the system from different viewpoints by analysing PA of the ISS.

3.Unification of the requirements, respective viewpoints towards the system. As a result, two conceptual models of the PA are formed – a generalized and a detailed one.

4. Integration of the created conceptual models.
5. Construction of a new object-oriented design model as a result of the transformation of the conceptual model of PA
6. Final construction of two new models – implementation model (object-oriented) and simulation model (agent-based) from the design model.

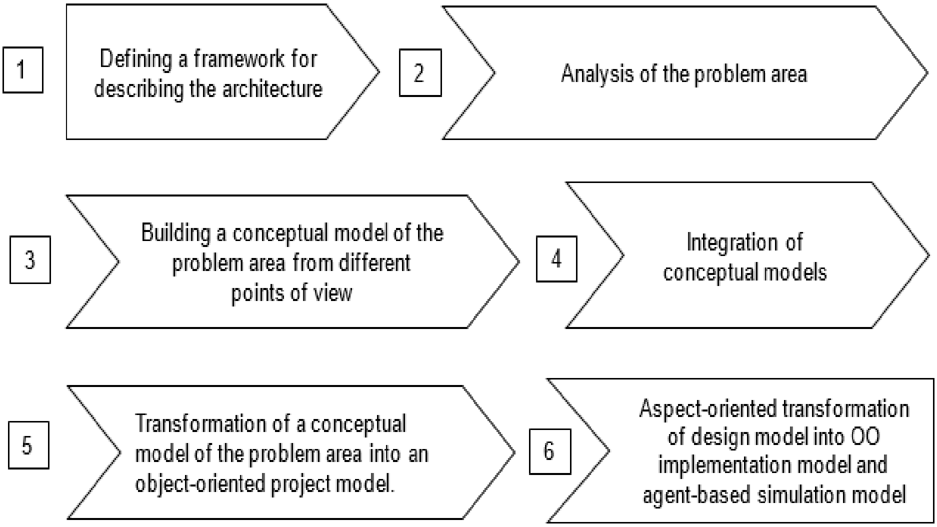
1
Defining a framework for describing the architecture
2
Analysis of the problem area
3
Building a conceptual model of the problem area from different points of view
4
Integration of conceptual models
5
Transformation of a conceptual model of the problem area into an object-oriented project model.
6
Aspect-oriented transformation of design model into OO implementation model and agent-based simulation model

Figure 1: Method for information security system development.

Through the method for development of ISS in organizations, an unlimited number of viewpoints can be defined, reflecting the requirements of the various interested parties (stakeholders). Such are, for example:

- Viewpoint Risk analysis - the requirements for ISS are determined after the risk analysis;
- Information processing perspective – takes into account the main types of data (data-in-motion, data-in-use and data-at-rest).
- Communication viewpoint - takes into account the types of communication in the ISS, determining the priorities in the protection of information;
- A technological perspective. It brings together the technologies and protection platforms used, together with different approaches such as object-oriented approach and agent approach;
- Information Security Perspective - brings together some basic IS concepts such as Vulnerabilities, Sources, Threats and Motivation. This includes the main approaches for implementing IS in organizations;

In the next section, we take a detailed look at the Information Security Perspective.

Fig.2 shows a conceptual model of an attack from the Information Security Viewpoint and related concepts such as "Incident," "Breach," "Vulnerability," "Threats," "Threat Sources," and "Threat Agent":

Information Security Perspective

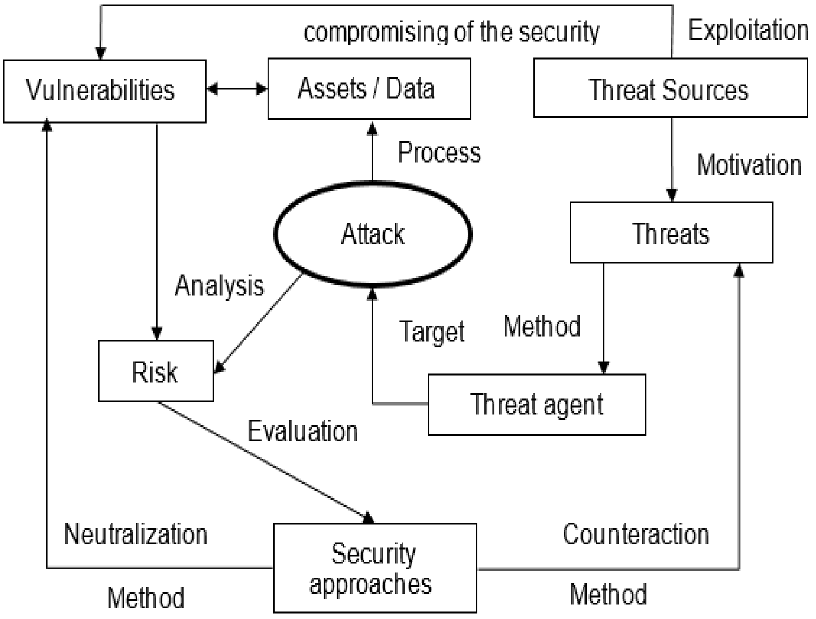

Figure 2: Basic IS concepts.

- "Incident" is an event compromising the Confidentiality, Integrity or Availability of Information Assets.
- In "Breach" we have an incident leading to a confirmed disclosure of data to an unauthorized party.[12, 13]
- "Vulnerability" is a weakness of the relevant asset or system, which is used by a threat source to achieve certain goals - a security breach or a violation of security procedures.[10, 13, 15, 1]
- "Threat" is the ability of the threat source to exploit a specific vulnerability, which leads to a security breach, data destruction, service interruption or violation of security procedures.[10, 11, 14, 16]

- "Threat Agent" – A threat agent is any person who acts or has the power to act, cause, transmit, or sustain a threat.
- "Threat Source" – The cause of a threat to information security.
- "Attack" – Any attempt to gain unauthorized access to an information asset through a targeted action that exploits a specific vulnerability from the threat source and commits a security breach resulting in a security incident. The goal of the attack is usually the unauthorized alteration, theft or destruction of informational or physical assets.[13, 14]

One of the most important components of risk analysis is threat assessment. It allows the protection of vital (critical) assets and resources, reducing the likelihood that they will be ignored.

Threats, Vectors, Targets, Threat Nature

Successfully countering threats requires an analysis that considers the possible elements of the threat and their impact. Threats in an information environment are related to specific vulnerabilities of the environment through which the source and, respectively, the threat agent can carry out an attack on the assets. Threats vary in their source, direction, nature, and outcome. A number of factors should be taken into account for their assessment: [12]

- Sources and threat agents;
- Motivation of threat agents;
- Threat vector;
- Nature of the threat;
- Targets of the threat;
- Impact of the threat.

The direction or vector of the threat is determined by the threat source and the path to reach the target. Such, for example, can be an attack by a hacker on a corporate network—the so-called "fishing"—an email or advertisement with a link to a malicious page sent to an employee. To identify potential threat vectors, a list of different types of threats, their source, and their target can be compiled (Table 1) using any combination of the three possible methods.

According to the direction (vector), the threats can be divided into external and internal.

External Threats

When the attack is from the outside and is directed against the information infrastructure of the organization, we have an External threat. In the case of external threats, the attacking party uses the principle of the weakest link - looking for gaps in the defence through which it is possible to penetrate the internal network. Next is taking control of information assets. As an example can be given DoS and DDoS attacks, Worms, Trojans, Botnets, Code Injection Attacks, Remote File Inclusion, and Exploit-driven attacks.

Table 1. Types of threats, sources, and targets.

Threat	Source	Target
Abuse	Employee	Intellectual property (IP)
Denial of service	Consultant	Personally Identifiable Information
Interruption	Supplier	Trade secret
Theft	System integrator	Personal Health Information
Exposure	Reseller	Credit card numbers
Data loss	Service provider	Financial information
Partial deletion	Hygiene staff	Social Security Numbers
Complete deletion	Insider	Documents
Unauthorized change	External support	Data
Illegal addition	Terrorists	Computer
Espionage	Internet attack	Network
Fraud	Software bug	Operating system
Identity spoofing	Malware	Applications
Malfunction	Accident	Voice communication
Error	Natural causes	Confidentiality
Physical impact	Time	Productivity

Internal Threats

When an insider to the organization, such as an employee, partner, or supplier with authorized access to sensitive information or system, abuses that access in violation of the accepted information security policy, leading to negative consequences for the organization, an incident occurs, which is classified as an insider threat. Abuse can be intentional or accidental. Insider threats are unpredictable and pose a serious challenge to traditional IT security measures. Insider threats can be attributed to incidents such as electronic identity theft, negligent behaviour by employees and outside contractors, malicious users, and overly strict security policies – "Security Fatigue."

According to their source, insider threats can be divided as follows:

Humans as an Insider Threat

Due to their tense daily lives, employees may become careless in their daily work, leading to security incidents. On the other hand, it is possible for them to intentionally violate the security policy and cause harm, as well as become the target of a hacker attack. Employees only pose a serious insider threat if they have access to sensitive information or systems critical to the organization's security. It is, therefore, critical to classify different types of users and profile them according to the risk they pose to the organization. The following categories of employees can be distinguished:

- Ordinary users with access to sensitive data.

- Privileged users – users with full access to the organization's resources, for example, system administrators
- External suppliers - suppliers external to the company, having access to its resources;

Ordinary users pose the greatest security risk to the organization due to their larger numbers compared to those of privileged and external vendors, which results in a higher overall security risk. Unlike the other categories of employees, ordinary users also carry a greater risk due to the lack of knowledge and skills to prevent accidents.[13] Therefore, in the information security policy in modern organizations, in addition to technical, organisational, and legal measures, employee training to increase their information security awareness is needed,[18, 14, 15] as well as the provision of modern training environments,[16] are mandatory.

User Activity

The most common insider threat vector is caused by the diverse daily activity of employees, consisting of a huge number of actions and operations. This makes it virtually impossible to detect unauthorized or risky activities. For this purpose, it is necessary for the organization to have modern means of information protection, monitoring, and possibly blocking suspicious actions that carry the risk of leakage of sensitive information, regardless of the type of threat - internal or external.

Business Applications

Business applications used by employees on a daily basis are a serious source of risks because of their access to sensitive data. In addition to specialized business applications, many additional applications are used in everyday work - office suites, cloud services, communication applications and many others. They represent a source of high risk for the organization.

Threat Sources, Agents, and Motivation

A "Threat agent" is any organization, group, or individual that can cause or maintain a threat to the organization's information assets. Threat agents carry out attacks by exploiting system vulnerabilities. By its nature, the damage can be alteration, leaking or deleting data, taking control of information systems, exploiting information assets, blocking the normal operation of business-critical systems, etc.[1, 10, 16] The sources of threat and their motivation are different in nature, but most often they are related to the human factor.

Some of the typical cyber threat agents are shown in Table2:

Hackers and Hacktivists. Traditionally, hackers aim to compromise or destroy an organization's IT resources or seek financial gain by stealing sensitive information. Hacktivism is a new trend among threat actors. Hacktivists are socially or politically motivated individuals who use attacks on information systems to protest or promote a particular cause. Their usual target is public websites of media and government institutions.

Cybercriminals. These types of threat agents are highly skilled and hostile in nature. Their motivation is financial.

Cyber-Terrorists. The motivation of terrorists is usually political or religious. Their preferred targets are objects of the critical infrastructure that have the potential to cause serious harm and corresponding impact on society.

Corporations. The motivation of this type of agents is to steal know-how, commercial, and financial information. Corporations possess significant resources of a technological and human nature that make them very dangerous.

Table 2. Threat agents and their motivation.

Threat Agent	Motivation	Method	Organization
Hackers, Hacktivists	Challenge, Protest Cause	Social engineering, Penetration, Fishing	Commercial, Administrative, Public
Cybercriminals	Destruction, Disclosure of information, Profit, Deceive	Computer Crime, Identity theft, Interception, Fraud, Misuse, Penetration	Commercial, Manufacture, Administrative, Public
Cyber terrorists	Extortion, Destruction, Exploitation, Revenge.	Info warfare, System attack, Penetration, System tampering.	Commercial, Manufacture, Scientific, Administrative, Public
Corporations	Economic Advantage, Industrial Espionage	Data Theft, Social engineering, Penetration	Commercial, Manufacture, Scientific
Insiders	Profit, Extortion, Revenge	Data Theft, Abuse, Access, Sabotage	Commercial, Manufacture, Administrative

Unscrupulous employees. These are usually employees with access to critical resources for the organization. They are particularly dangerous due to the fact that they are already in a protected environment and have practically legally overcome all traditional protection measures. New methods are needed for their prevention, such as Data Leak Prevention (DLP) platforms. These agents have a variety of motivations – negligence, displeasure, malice, and financial gain.

Governments. These are the most powerful types of threat agents. Their motivation is geo-political and economic or a combination of both. Their goals are securing a strategic advantage, dominance in certain sectors, and advancing state interests. Detailed information about this type of agents can be found in specialized lists and libraries such as NIST Threat Sources, Intel Threat Library, FAIR Threat Communities, VERIS Threat Agent Categories, OWASP Threat Agent Groups, etc.[14]

Attacks and Countermeasures

An attack is a process where the threat source takes a targeted action that exploits a specific vulnerability to compromise the security of an asset through disclosure, alteration, theft, destruction, unauthorized access, or unauthorized use. The attack is a sequence of purposeful actions performed by the threat source by exploiting a specific vulnerability. The purpose is to compromise the security of an asset by destroying, altering, or unauthorized access to the asset. The different types can be categorized into the following categories:

- Interception;
- Interruption;
- Modification;
- Fabrication.

To neutralize the threats, a set of measures called approaches to information security (AIS) can be used. AIS can be a procedure, process, or group of actions taken to protect information assets, neutralize threats, as well as recovery actions. These approaches can be both technological and organizational and are applied in accordance with the specifics of the organization's activities. AIS can be grouped into several categories according to the time of their action:

- Preventive – Eliminate potential threats before they take advantage of a given vulnerability;
- Detectable – Detect and warn of attacks in real-time, at the moment of their occurrence;
- Deterrence - Prevents external attacks before they are deployed.
- Corrective – Restore data integrity and other affected assets;
- Restorative – Restore the availability of attacked and disrupted services;

- Compensatory – Compensate the consequences of successful attacks. They are used in a multi-layered security strategy.

Conclusions

Of particular importance in the design of an efficient ISS is the consideration of all stakeholders. In addition to technological requirements, the modern dynamics of an organization's work requires compliance with a number of regulations and good practices. In turn, their compliance entirely depends on the working environment of the organization, its employees, their loyalty and good faith. This is the so-called human factor. The behaviour of employees in relation to the adopted information security policy cannot be predicted, therefore it is necessary to foresee a number of measures already in the process of designing the system. These include both technical solutions and organizational processes and procedures. The object of the present study is the clarification of the human factor as a threat to the system. The authors anticipate expanding the topic through future publications with the main topic of countering human threats. The results will be used to enhance employee education.

Acknowledgement

This work was supported by the NSP DS program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. D01-74/19.05.2022.

References

[1] Jason Andress, "The basics of information security: understanding the fundamentals of InfoSec in theory and practice," Elsevier Inc., 2011.

[2] Zlatogor Minchev and Ivan Gaydarski, "Cyber Risks, Threats and Protective Measures Related to COVID-19," *CSDM Views* 37, 2020.

[3] Antoni Olivé, "Conceptual Modeling of Information Systems," *Springer*, January 2007, https://doi./10.1007/978-3-540-39390-0.

[4] Varuni Mallikaarachchi, "Data Modeling for System Analysis," Information Systems Analysis – IS 6840, University of Missouri, St. Louis, 2010.

[5] Ivan Gaydarski, Zlatogor Minchev, and R. Andreev, "Model Driven Architectural Design of Information Security System," Advances in Intelligent Systems and Computing," In: Madureira A., Abraham A., Gandhi N., Silva C., Antunes M. (eds) *Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition* (SoCPaR 2018), *Springer*, 2019, https://doi./10.1007/978-3-030-17065-3_35, 349-359.

[6] Rich Hilliard, David Emery, and Mark Maier, "ANSI/IEEE 1471 and Systems Engineering," *Systems Engineering* 7, no. 3 (2004): 257–270, https://doi./10.1002/sys.20008.

[7] IEEE SA, “IEEE 1471-2000: IEEE Recommended Practice for Architectural Description for Software-Intensive Systems,” https://standards.ieee.org/ieee/1471/2187/, accessed September 05, 2024.

[8] ISO, “ISO/IEC/IEEE 42010:2022 – Software, systems and enterprise — Architecture description,” Edition 2, 2022, https://www.iso.org/standard/74393.html.

[9] Pericherla Satya Suryateja, “Threats and Vulnerabilities of Cloud Computing: A Review,” *International Journal of Computer Sciences and Engineering* 6, no. 3 (2018).

[10] Yuri Diogenes and Erdal Ozkaya, Cybersecurity – Attack and Defence Strategies (Packt Publishing Ltd., 2019).

[11] Mark Ciampa, *Security+ Guide to Network Security Fundamentals*, 4th Edition (Course Technology, Cengage Learning, 2015).

[12] Radoslav Miltchev and Neda Chehlarova, “Development of Digital Competencies and Skills in the Field of Use of Cloud Services and Electronic Communication,” *Science, Engineering & Education* 5, no. 1 (2020): 41-50.

[13] Willian Dimitrov, Katia Rasheva-Yordanova, Oleg Konstantinov, Kristina Bosakova, and Viktoriya Angelova, “Toward overcoming the disproportion between the demand for professionals and the provision of training in cybersecurity,” In *EDULEARN19 Proceedings, 11th International Conference on Education and New Learning Technologies*, 13 July, 2019, pp. 1656–1664, https://doi./10.21125/edulearn.2019.0485.

[14] Valentina Terzieva, Svetozar Ilchev, and Edita Djambazova, “Integrated Intelligent Educational Environment – Opportunities for STEM Education,” *IFAC-PapersOnLine* 58 (2024): 94-99, https://doi./10.1016/j.ifacol.2024.07.132.

About the Authors

Dr. Ivan **Gaidarski** is a researcher on communications and computer technology at the Laboratory of Unmanned Robotic Systems in the Institute of Robotics, Bulgarian Academy of Sciences.
https://orcid.org/0000-0002-4979-445X

Anastas **Madzharov** received a Ph.D. degree in Navigation Systems in 1991 and became Associate Professor in “Dynamics, Ballistics and Control of Aircraft” in 2000. From 2000 to 2016, Dr. Madzharov led the Electronics, Automation, and Information Technologies department of the Bulgarian Air Force Academy and lectured on “Inertial Navigation System,” “System Identification,” and “Optimal and Adaptive Control.” Currently, he is an Associate Professor at the Laboratory of Unmanned Robotic Systems in the Institute of Robotics, Bulgarian Academy of Sciences. https://orcid.org/0000-0002-6282-617X